IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:

Steve VLCAN, et al.

Serial No.:	**10/015,886**	Art Unit:	**2431**
Filed:	**December 17, 2001**	Examiner:	**MOORTHY, Aravind K.**

For: **SYSTEM AND METHOD FOR AUTOMATICALLY DETECTING AND THEN SELF-REPAIRING CORRUPT, MODIFIED OR NON-EXISTENT FILES VIA A COMMUNICATION MEDIUM**

FILED ELECTRONICALLY

U.S. Patent and Trademark Office
Customer Window, Mail Stop, Appeal Brief - Patents
Randolph Building
401 Dulany Street
Alexandria, VA 22314

APPEAL BRIEF

Dear Sir:

This is an Appeal Brief under 37 C.F.R. § 41.37 in response to a Final Office Action mailed October 16, 2008 and an Advisory Action mailed on January 14, 2009. Each of the topics required by Rule 41.37 is presented herewith and is labeled appropriately. The Notice of Appeal was filed on January 16, 2009.

(1) Real Party in Interest

The real party in interest is Citibank, N.A., 909 Third Avenue, 15th Floor, New York, NY 10022.

(2) Related Appeals and Interferences

Appellants are unaware of any related appeals and interferences.

(3) Status of Claims

Claims 1-3, 5-11, and 13-18 are pending in this application. Claims 1-3, 5-11, and 13-18 stand under final rejection. Claims 1-3, 5-11, and 13-18 are hereby appealed.

(4) Status of Amendments

There are no outstanding amendments.

(5) Summary of the Claimed Subject Matter

This summary of claimed subject matter is a concise explanation of the subject matter defined in independent claims 1 and 10. This is merely meant to be a summary and is in no way intended to limit the pending claims.

In one embodiment, as recited in claim 1, a method for maintaining the integrity of a file at a remote location via a communication medium, comprises the steps of performing an integrity check on the file by an integrity module (Para. [0039], ref. num. (202)); redirecting to an install module by a redirect module if said integrity check fails (Para. [0042], ref. num. (208)); and reinstalling the file by the install module at the remote location via the communication medium, thereby maintaining the integrity of the file (Para. [0043], ref. num. (210)). The step of redirecting to the install module comprises the steps of modifying an address of the install module by the redirect module to include a parameter to indicate the remote location of the file (Para. [0050], ref. num. (402)); producing a request by an authentication module based on the modified address that indicates the remote location of the file (Para. [0052], ref. num. (406)); and communicating the request by the authentication module to the install module in a login page that instantiated the file at the remote location (Para. [0053], ref. num. (408)).

In another embodiment, as recited in claim 10, a system for maintaining the integrity of a file at a remote location via a communication medium, comprises an integrity module (Para. [0058], ref. num. (110)); a redirect module coupled to said integrity module via the communication medium (Para. [0058], ref. num. (114)); an install module coupled to said redirect module via the communication medium (Para. [0058], ref. num. (118)), wherein said integrity module performs an integrity check on the file (Para. [0032], ref. num. (110)), and wherein said redirect module redirects to said install module when the integrity check fails and modifies an address of the install module to include a parameter to indicate the remote location of the file (Para. [0050], ref. num. (402)); and an authentication module coupled to the redirect module which authentication module produces a request based on the modified address that indicates the remote location of the file and communicates the request to said install module in a login page that instantiated the file at the remote location (Para. [0052], ref. num. (107)), and wherein said install module reinstalls the file at the remote location, thereby maintaining the integrity of the remote file (Para. [0043], ref. num. (118)).

(6) Grounds of Rejection to be Reviewed on Appeal

A. Whether the Examiner's rejection of claims 1-3, 6, 7, 9-11, 14, 15, 17 and 18 under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent Publication No. 2002/0069363 to Winburn ("Winburn") is proper.

B. Whether the Examiner's rejection of claims 5 and 13 under 35 U.S.C. § 103(a) as being unpatentable over Winburn as applied to claims 1 and 10 above, and further in view of U.S. Patent No. 5,991,760 to Gauvin et al. ("Gauvin") is proper.

C. Whether the Examiner's rejection of claims 8 and 16 under 35 U.S.C. § 103(a) as being unpatentable over Winburn as applied to claims 1 and 10 above, and further in view of U.S. Patent No. 5,909,429 to Satyanarayana et al. ("Satyanarayana") is proper.

(7) Argument

A. The Examiner's rejection of claims 1-3, 6, 7, 9-11, 14, 15, 17 and 18 under 35 U.S.C. § 102(e) as being anticipated by Winburn is improper.

Winburn is directed to detecting whether a protected data file has been changed and, if so, restoring the protected data file using a backup data file. See, e.g., Para. [0004]. Winburn uses an algorithm, such as a hashing algorithm, to create an identifier for the protected data file. Para. [0008]. A test identifier can be created from a protected data file and, if it does not match the previous identifier, then the protected data file has been modified. *Id.* If the protected data file has been modified, Winburn uses an authentic backup file to restore the protected data file. Paras. [0008]-[0009]. The authentic backup file is camouflaged to prevent access or modification of the authentic backup file. Para. [0009]-[0010]. Indicia for the location of the authentic backup file is stored in an active or RAM memory of a data processor. Para. [0011]. Winburn touts the location of the indicia in the active or RAM memory as a mechanism for further camouflaging, and Winburn disparages the storage of indicia in a static or disk memory. Para. [0011].

In contrast, as recited in claims 1 and 10, if a file fails an integrity check, then the remote file is reinstalled. As recited in the specification, "Redirect module 114 works with install module 118 to inform it of the location of the remote file that failed the integrity check." Para. [0033]; *see also* para. [0050]. "Once a remote file has failed the integrity check, then it is reinstalled at the remote location." Para. [0034]. Accordingly, Winburn does not disclose "modifying an address of the install module by the redirect module to include a parameter to indicate the remote location of the file," as recited in claim 1 and similarly recited in claim 10. Further, Winburn does not disclose "reinstalling the file by the install module at the remote location via the communication medium," as recited in claim 1 and similarly recited in claim 10.

Winburn is not modifying an address of an install module to indicate the remote location of a file. Instead, Winburn uses an indicia in an active or RAM memory in order to camouflage the location of a backup file. As a result, Winburn cannot modify an address of an install module, because an install module is not resident in active or RAM memory. As recited in the specification, the install module is associated with a web/application server (106). *See*, *e.g.*, Para. [0034].

Further, Winburn is not checking the integrity of a remote file or reinstalling a remote file. Winburn's protected data file is not a physically remote file, and the Examiner has repeatedly failed to provide a prima facie case supporting such an assertion. Winburn recites two data files, including a protected data file and an authentic backup file. There is no disclosure that the protected data file is remotely located, so Winburn does not adequately establish a prima facie case that the protected data file is a file that is reinstalled at a remote location. Similarly, the authentic backup file cannot be a reinstalled file because the authentic backup file is not reinstalled. Instead, the authentic backup file is used to reinstall the protected data file.

The address of the install module is modified to include a parameter to indicate the remote location of the file. Winburn, in contrast, has no need to indicate the remote location of the protected data file because it is already known. In order to increase security, Winburn camouflages indications of the location of the authentic backup file. As a result, Winburn does not disclose modifying any parameters indicating a remote location of its protected data file.

Additionally, Winburn does not disclose "communicating the request by the authentication module to the install module in a login page that instantiated the file at the remote location," as recited in claim 1 and similarly recited in claim 10. First, as discussed above, Winburn does not disclose a remote location and, thus, a file at the remote location. Second, Winburn does not disclose "a login page that instantiated the file at the remote location." The Examiner asserts that Para. [0031] of Winburn discloses this element, however, the paragraph is directed to restoring a protected file and does not disclose any method of authentication, such as a login page.

Therefore, Winburn does not anticipate independent claims 1 and 10 and similarly does not anticipate claims 2, 3, 6, 7, 9, 11, 14, 15, 17, and 18 depending on claims 1 and 10, and which recite further specific elements that have no reasonable correspondence with Winburn. Thus, it is respectfully requested that the rejection under 35 U.S.C. § 102(e) be reversed.

B. The Examiner's rejection of claims 5 and 13 under 35 U.S.C. § 103(a) as being unpatentable over Winburn as applied to claims 1 and 10 above, and further in view of Gauvin is improper.

Although the Examiner recites the § 103(a) rejections over Winburn as applied to claims 1 and 10, the Examiner recites U.S. Patent No. 6,779,003 to Midgley. Because the Examiner rejects claims 1 and 10 as being anticipated by Winburn, the undersigned representative understands the § 103(a) rejections to be over Winburn instead of Midgley. The undersigned representative requested clarification of this rejection, but this concern was not addressed. Accordingly, the undersigned representative has interpreted these rejections in view of Winburn.

Claims 5 and 13 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Winburn as applied to claims 1 and 10 above, and further in view of Gauvin. This rejection is respectfully traversed. For the reasons set forth above with respect to claims 1 and 10, Winburn does not establish a *prima facie* case of obviousness with respect to claim 1, because Winburn does not teach or suggest each and every element. Additionally, for at least the reasons set forth above with respect to claims 1 and 10, Gauvin fails to cure the deficiencies of Winburn. Because claims 5 and 13 depend on claims 1 and 10, it is respectfully submitted that claims 5 and 13 are also in condition for allowance.

Additionally, Winburn and Gauvin fail to teach or suggest "generating a reinstallation web page, by the install module, based on a request from the remote location," as recited in claim

5 and similarly recited in claim 13. Although Gauvin recites downloading via a client browser, Gauvin does not teach or suggest "generating a reinstallation web page." The Examiner's citation to col. 6, lines 17-60 of Gauvin does not support the Examiner's assertion. In fact, Gauvin recites downloading additional websites that are reviewed only when the client computer is disconnected from the network. Col. 9, lines 1-14. Such websites, as a result, cannot function as a reinstallation web page when reviewed after the client computer is no longer connected to the network. Therefore, neither Winburn nor Gauvin teach or suggest each and every element of claims 5 and 13.

Therefore, the undersigned representative respectfully requests that the rejection of claims 5 and 13 be reversed.

C. The Examiner's rejection of claims 8 and 16 under 35 U.S.C. § 103(a) as being unpatentable over Winburn as applied to claims 1 and 10 above, and further in view of Satyanarayana is improper.

Claims 8 and 16 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Winburn as applied to claims 1 and 10 above, and further in view of Satyanarayana. This rejection is respectfully traversed. For the reasons set forth above with respect to claims 1 and 10, Winburn does not establish a *prima facie* case of obviousness with respect to claim 1, because Winburn does not teach or suggest each and every element of claim 1. Additionally, for at least the reasons set forth above with respect to claims 1 and 10, Satyanarayana fails to cure the deficiencies of Winburn. Because claims 8 and 16 depend on claims 1 and 10, it is respectfully submitted that claims 8 and 16 are also in condition for allowance.

Therefore, the undersigned representative respectfully requests that the rejection of claims 8 and 16 be reversed.

(8) Claims Appendix

1. (Previously Presented) A method for maintaining the integrity of a file at a remote location via a communication medium, comprising the steps of:

performing an integrity check on the file by an integrity module;

redirecting to an install module by a redirect module if said integrity check fails, wherein the step of redirecting to the install module comprises the steps of:

modifying an address of the install module by the redirect module to include a parameter to indicate the remote location of the file;

producing a request by an authentication module based on the modified address that indicates the remote location of the file; and

communicating the request by the authentication module to the install module in a login page that instantiated the file at the remote location; and

reinstalling the file by the install module at the remote location via the communication medium, thereby maintaining the integrity of the file.

2. (Previously Presented) The method of claim 1, wherein the step of performing the integrity check comprises the steps of:

using an algorithm on the file to produce a remote value;

communicating the remote value to the integrity module via the communication medium;

using the algorithm on a mirror file to produce a secure value, wherein the mirror file is a valid copy of the file; and

communicating that the integrity check passed if the remote value and the secure value are equivalent.

3. (Original) The method of claim 2, wherein said algorithm is a hash algorithm.

4. (Cancelled)

5. (Original) The method of claim 1, wherein the step of reinstalling the remote file comprises the steps of:

generating a reinstallation web page, by the install module, based on a request from the remote location;

communicating the reinstallation web page, via the communication medium, to the remote location; and

reinstalling the remote file at the remote location.

6. (Original) The method of claim 1, wherein the communication medium is the Internet.

7. (Original) The method of claim 1, wherein the communication medium is a local network.

8. (Original) The method of claim 1, wherein the communication medium is a wireless network.

9. (Original) The method of claim 1, wherein the remote location is an authentication control component.

10. (Previously Presented) A system for maintaining the integrity of a file at a remote location via a communication medium, comprising:

an integrity module;

a redirect module coupled to said integrity module via the communication medium;

an install module coupled to said redirect module via the communication medium, wherein said integrity module performs an integrity check on the file, and wherein said redirect module redirects to said install module when the integrity check fails and modifies an address of the install module to include a parameter to indicate the remote location of the file; and an authentication module coupled to the redirect module which authentication module produces a request based on the modified address that indicates the remote location of the file and communicates the request to said install module in a login page that instantiated the file at the remote location, and wherein said install module reinstalls the file at the remote location, thereby maintaining the integrity of the remote file.

11. (Original) The system of claim 10, further comprising an authentication control component that uses an algorithm on the file to produce a remote value, wherein said integrity module uses the algorithm on a mirror file to produce a secure value, wherein the mirror file is a valid copy of the file, and wherein said integrity module compares the remote value and the secure value to determine whether the integrity check has been passed.

12. (Cancelled)

13. (Original) The system of claim 10, wherein said install module generates a reinstallation web page based on a request from the remote location to be used to reinstall the remote file at the remote location.

14. (Original) The system of claim 10, wherein the communication medium is the Internet.

15. (Original) The system of claim 10, wherein the communication medium is a local network.

16. (Original) The system of claim 10, wherein the communication medium is a wireless network.

17. (Original) The system of claim 10, wherein the remote location is an authentication control component.

18. (Original) The system of claim 11, wherein the algorithm is a hash algorithm.

(9) Evidence Appendix

None.

(10) Related Proceedings Appendix

None.

CONCLUSION

The undersigned representative respectfully submits that this application is in condition for allowance, and such disposition is earnestly solicited. Applicants respectfully request that the final rejections by the Examiner be reversed. Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, to Deposit Account 50-4402, and please credit any excess fees to such deposit account.

Respectfully submitted,

Date: __June 12, 2009_____
KING & SPALDING LLP
1700 Pennsylvania Ave., NW
Washington, DC 20006
(202) 626-8980

By: _*/Eric Sophir, Reg. No. 48,499/*____
Eric L. Sophir
Registration No. 48,499